

Incentives- Liability/Safe Harbor

Working Group

Coordinators: Ty Sagalow, AIG and Larry Clinton Internet Security Alliance

Incentives Principles

The Sub-Group determined that the following principals are best positioned to accomplish the Mission of the group:

1. Positive incentives are likely to generate long term and more effective results in cyber-security. This will ultimately increase consumer and business confidence in the use of advanced technology, promote homeland security and result in economic benefits for all Americans.
2. Positive incentives are likely to be an effective means of implementing a comprehensive cyber security risk management program because it would:
 - Leverage private industry's ability to innovate and maintain the tools necessary for effective cyber- security.
 - Apply to the global economy due to international nature of major corporations.
 - Respond to change in technology.
 - Encourage executive buy- in due to inherent advantages to a "return on investment" approach.
 - Promote market-based incentive programs that are more readily designed to apply to the broad cross-section of entities who use and must protect the cyberspace.
 - Compliment the existing sector specific initiatives.
3. Duplicative and conflicting international, national, state and local regulatory requirements create disincentives to effective cyber-security.
4. Traditional regulatory structures are likely to be ineffective and potentially unproductive because:
 - The international nature of the cyber security issue cannot be adequately addressed by national legislation.
 - The rapid and continuing change of cyberspace and the cyber security threat demands flexible solutions that can be quickly adapted to new circumstances. This is inconsistent with the nature of the traditional regulatory structure.
 - The traditional regulatory method usually involves a public notice and comment procedure. In this case, the use of a public disclosure process could inadvertently provide a road map to terrorists and other parties intent on causing harm to cyber-security systems.
 - The political process encourages compromise rather than maximum effectiveness and could result in an inefficient program that could yield a false sense of security.
 - Government regulation of technology may blunt innovation resulting in less consumer choice, economy and security.